Axcelera Ltd (Axcelera) Data Protection Policy

Contents

1. **Introduction**

This policy outlines the responsibilities of Axcelera Ltd (Axcelera), a registered company in England under number 15353435, with its registered office at 124 City Road, London, United Kingdom, EC1V 2NX (“the Company”), concerning data protection and the rights of individuals such as customers, suppliers, team members, consultants, agents, contractors, employees, and other business contacts (“data subjects”) with regard to their personal data under The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (“GDPR”).

According to the GDPR, "personal data" is defined as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be directly or indirectly identified, particularly by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This policy outlines the Company's obligations concerning the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles stated herein must be adhered to at all times by the Company, its employees, team members, consultants, agents, contractors, or other parties working on behalf of the Company (“Users”).

The Company is dedicated not only to complying with the letter of the law but also to upholding the spirit of the law. It places significant emphasis on the proper, legal, and equitable handling of all personal data, demonstrating respect for the legal rights, privacy, and trust of all individuals with whom it engages.

2. **The Data Protection Principles**

This Policy is designed to ensure compliance with the GDPR. The GDPR outlines the following principles that must be adhered to by any party handling personal data:

2.1 Processed lawfully, fairly, and transparently in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Additional processing for archiving purposes in the public interest, scientific or historical research, or statistical purposes is not considered incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure prompt erasure or rectification of inaccurate personal data concerning the data subject.

2.5 Kept in a form allowing identification of data subjects for no longer than necessary for the purposes of processing. Personal data may be stored for extended periods if processed solely for archiving purposes in the public interest, scientific or historical research, or statistical purposes, subject to the implementation of appropriate technical and organisational measures as required by the GDPR to safeguard the rights and freedoms of the data subject.

2.6 Processed in a manner ensuring the appropriate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, using suitable technical or organisational measures.

3. **The Rights of Data Subjects**

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12).

3.2 The right of access (Part 13);

3.3 The right to rectification (Part 14);

3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);

3.5 The right to restrict processing (Part 16);

3.6 The right to data portability (Part 17);

3.7 The right to object (Part 18); and

3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. **Lawful, Fair and Transparent Data Processing**

4.1 The GDPR aims to ensure the lawful, fair, and transparent processing of personal data, without adversely affecting the rights of the data subject. The GDPR specifies that processing of personal data is considered lawful if at least one of the following conditions applies:

4.1.1 The data subject has provided consent to the processing of their personal data for one or more specific purposes.

4.1.2 The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before entering into a contract.

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject.

4.1.4 The processing is necessary to protect the vital interests of the data subject or another natural person.

4.1.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

4.1.6 The processing is necessary for the legitimate interests pursued by the data controller or a third party, unless overridden by the fundamental rights and freedoms of the data subject, especially when the data subject is a child.

4.2 The company does not hold personal data considered "special category data" (also known as "sensitive personal data")—such as data concerning race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation. If it did, at least one of the following conditions would need to be met:

4.2.1 The data subject has given explicit consent to process such data for one or more specified purposes (unless prohibited by UK law).

4.2.2 The processing is necessary to fulfil obligations and exercise specific rights of the data controller or data subject in the field of employment, social security, and social protection law, as authorised by UK law or a collective agreement with appropriate safeguards.

4.2.3 The processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

4.2.4 The data controller is a foundation, association, or other non-profit body with political, philosophical, religious, or trade union objectives, and the processing is carried out in the course of its legitimate activities. It must relate solely to members or former members of that body or persons with regular contact in connection with its purposes, and the personal data is not disclosed outside the body without the consent of the data subjects.

4.2.5 The processing relates to personal data explicitly made public by the data subject.

4.2.6 The processing is necessary for the conduct of legal claims or when courts are acting in their judicial capacity.

4.2.7 The processing is necessary for substantial public interest reasons under UK law, proportionate to the pursued aim, respecting the essence of the right to data protection, and providing suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

4.2.8 The processing is necessary for purposes of preventative or occupational medicine, assessing employee working capacity, medical diagnosis, providing health or social care or treatment, or managing health or social care systems or services. This is based on UK law or pursuant to a contract with a health professional, subject to conditions and safeguards specified in Article 9(3) of the GDPR.

4.2.9 The processing is necessary for public interest reasons in public health, such as protecting against serious cross-border health threats or ensuring high standards of quality and safety in healthcare and medicinal products or medical devices. This is based on UK law, providing suitable and specific measures to safeguard the rights and freedoms of the data subject, particularly professional secrecy.

4.2.10 The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR. This is based on UK law, proportionate to the pursued aim, respecting the essence of the right to data protection, and providing suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

5. **Specified, Explicit, and Legitimate Purposes**

5.1 The Company engages in the collection and processing of personal data as outlined in the Data Retention Schedule found in the Directory of Data, Assets, Risk, Systems & Retention Schedule. This encompasses:

5.1.1 Personal data collected directly from data subjects; and

5.1.2 Personal data obtained from third parties.

5.2 The Company strictly gathers, processes, and retains personal data solely for the explicit purposes delineated in Part 34: Schedule 1: Lawful Reasons for Processing, or for other purposes explicitly permitted by the GDPR.

5.3 Data subjects are consistently kept informed about the purpose or purposes for which the Company utilises their personal data. For additional details on maintaining data subject awareness, please consult Part 12.

6. **Adequate, Relevant, and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in part 34: *Schedule 1: Lawful Reasons For Processing*.

7. **Accuracy of Data and Keeping Data Up-to-Date**

7.1 The Company is committed to maintaining the accuracy and currency of all personal data collected, processed, and held by it. This encompasses, among other things, rectifying personal data upon the request of a data subject, as outlined in Part 14.

7.2 The accuracy of personal data will be verified during its collection and periodically thereafter. If any personal data is discovered to be inaccurate or outdated, prompt and reasonable measures will be taken to correct or erase the data as necessary.

8. **Data Retention**

8.1 The Company will not retain personal data beyond the necessary duration for the original purpose or purposes for which it was collected, held, and processed.

8.2 Upon the conclusion of the need for personal data, the Company will promptly take all reasonable measures to erase or dispose of it.

8.3 Comprehensive information about the Company's strategy for data retention, including specific retention periods for various types of personal data held by the Company, can be found in the Data Retention Policy available on the Directory of Data, Assets, Risk, Systems & Retention Schedule.

9. **Secure Processing**

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. **Accountability and Record-Keeping**

The Company's Data Protection Team is:

Michael Spyrou ***CEO***

10.1 The Company's Data Protection email address is: data@axcelera.co.uk

10.2 The implementation of this Policy and the monitoring of compliance with this Policy, as well as the Company's other data protection-related policies, the GDPR, and other applicable data protection legislation, shall be overseen by the Data Protection Team.

The Company will maintain internal records encompassing the following information related to personal data collection, holding, and processing:

10.2.1 The Company's name and details, along with those of its Data Protection Team and any relevant third-party data processors.

10.2.2 The purposes for which the Company collects, holds, and processes personal data.

10.2.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subjects to which that personal data pertains.

10.2.4 Details of any transfers of personal data to non-UK countries, including all mechanisms and security safeguards.

10.2.5 Information about the duration for which personal data will be retained by the Company (please consult the Company's Data Retention Policy).

10.2.6 Comprehensive descriptions of all technical and organisational measures adopted by the Company to ensure the security of personal data.

11. **Data Protection Impact Assessments**

11.1 The Company will conduct Data Protection Impact Assessments for all new projects and/or novel applications of personal data.

11.2 Oversight of Data Protection Impact Assessments will be carried out by the Data Protection Team, addressing the following aspects:

11.2.1 The type(s) of personal data to be collected, held, and processed.

11.2.2 The purpose(s) for which personal data will be utilised.

11.2.3 The Company's objectives.

11.2.4 How personal data will be employed.

11.2.5 The parties (internal and/or external) to be consulted.

11.2.6 The necessity and proportionality of the data processing in relation to its intended purpose(s).

11.2.7 Risks to data subjects.

11.2.8 Risks both within and to the Company.

11.2.9 Proposed measures to minimise and address identified risks.

12. **Keeping Data Subjects Informed**

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 When personal data is directly collected from data subjects, its purpose will be communicated to them at the time of collection.

12.1.2 When personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) If the personal data is used to communicate with the data subject, at the time of the first communication.

b) If the personal data is to be transferred to another party, prior to the transfer.

c) As soon as reasonably possible, and in any case, within one month after obtaining the personal data.

12.2 The provided information will include:

12.2.1 Company details, including contact information for the Data Protection Team.

12.2.2 The purpose(s) for collecting and processing the personal data, as detailed in Schedule 1 at the end of this policy, along with the legal basis justifying the collection and processing.

12.2.3 Legitimate interests, where applicable, upon which the Company justifies its collection and processing of personal data.

12.2.4 Categories of personal data collected and processed when not obtained directly from the data subject.

12.2.5 Details of third parties to whom the personal data will be transferred.

12.2.6 Information about the transfer of personal data to a third party outside the UK, including safeguards in place (refer to Part 28 of this Policy for further details).

12.2.7 Data retention details.

12.2.8 Data subject's rights under the GDPR.

12.2.9 Data subject's right to withdraw consent to the Company's processing of their personal data at any time.

12.2.10 Data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR).

12.2.11 Any legal or contractual requirement or obligation necessitating the collection and processing of personal data, along with consequences of failing to provide it.

12.2.12 Details of any automated decision-making or profiling using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. **Data Subject Access**

13.1 At any time, individuals have the right to make Subject Access Requests (SARs) to acquire information about the personal data held by the Company, its usage, and the reasons for such processing.

13.2 To initiate a SAR, individuals should use a Subject Request Form (SRF) and submit the form to the Company's Data Protection Team at data@axcelera.co.uk.

13.3 In general, responses to SRFs will be provided within one month of receipt. However, in instances of complex SRFs or a high volume of requests, this period may be extended by up to two months. The individual will be notified if such an extension is necessary.

13.4 The handling of all received SRFs will be overseen by the Company's Data Protection Team.

13.5 The Company does not charge a fee for processing standard SRFs. Nevertheless, for additional copies of information already provided to an individual and for requests considered manifestly unfounded or excessive, especially in cases of repetition, the Company reserves the right to charge reasonable fees.

14. **Rectification of Personal Data**

14.1 Data subjects have the right to request the Company to correct any of their personal data that is inaccurate or incomplete.

14.2 Data subjects seeking to make a data rectification request should do so using a Subject Request Form (SRF) and sending the form to the Company's Data Protection Team at data@axcelera.co.uk.

14.3 All SRFs received will be handled by the Company's Data Protection Team.

14.4 The Company does not impose a fee for processing standard SRFs. However, the Company reserves the right to charge reasonable fees for additional copies of information already supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly in cases of repetition.

14.5 The Company will correct the relevant personal data and notify the data subject of the rectification within one month of the data subject reporting the issue to the Company. This period may be extended by up to two months for complex requests. If additional time is needed, the data subject will be informed.

14.6 If any affected personal data has been disclosed to third parties, those parties will be informed of any rectification required for that personal data.

15. **Erasure of Personal Data**

15.1 Individuals have the right to request the Company to delete their personal data in the following circumstances:

15.1.1 It is no longer necessary for the Company to retain that personal data concerning the purpose(s) for which it was initially collected or processed.

15.1.2 The individual wishes to withdraw their consent to the Company holding and processing their personal data.

15.1.3 The individual objects to the Company holding and processing their personal data (with no overriding legitimate interest to allow the Company to continue) (refer to Part 18 of this Policy for further details regarding the right to object).

15.1.4 The personal data has been processed unlawfully.

15.1.5 The erasure of personal data is necessary for the Company to comply with a specific legal obligation.

15.2 Unless the Company has reasonable grounds to refuse personal data erasure, all erasure requests will be fulfilled, and the individual will be notified of the erasure within one month of receiving the request. The period may be extended by up to two months for complex requests, and the individual will be informed if additional time is needed.

15.3 Individuals wishing to make a data erasure request should do so using a Subject Request Form (SRF) and submit the form to the Company's Data Protection Team at data@axcelera.co.uk.

15.4 All received SRFs will be handled by the Company's Data Protection Team.

15.5 The Company does not charge a fee for processing standard SRFs. However, the Company reserves the right to charge reasonable fees for additional copies of information already provided to an individual and for requests deemed manifestly unfounded or excessive, especially in cases of repetition.

15.6 If any personal data to be erased in response to an individual's request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

16.1 Individuals may request that the Company stops processing the personal data it possesses about them. Upon receiving such a request, the Company will retain only the necessary amount of personal data concerning that individual (if any) to ensure that the specified personal data is not processed further.

16.2 Individuals wishing to make a data restriction request should use a Subject Request Form (SRF) and submit the form to the Company's Data Protection Team at data@axcelera.co.uk.

16.3 All received SRFs will be managed by the Company's Data Protection Team.

16.4 The Company does not impose a fee for processing standard SRFs. However, the Company reserves the right to charge reasonable fees for additional copies of information already supplied to an individual and for requests that are manifestly unfounded or excessive, especially in cases of repetition.

16.5 If any affected personal data has been disclosed to third parties, those parties will be informed of the applicable processing restrictions (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**

17.1 When individuals have provided their consent for the Company to process their personal data, or when processing is necessary for the performance of a contract between the Company and the individual, the GDPR grants individuals the right to receive a copy of their personal data and use it for other purposes, such as transmitting it to other data controllers.

17.2 To facilitate the right of data portability, the Company will provide all relevant personal data to individuals in the following format:

17.2.1 Password-protected files;

17.2.2 Where technically feasible and upon request by an individual, personal data will be sent directly to the required data controller, and the password will be sent to the individual.

17.3 Individuals wishing to make a data portability request should do so using a Subject Request Form (SRF) and sending the form to the Company's Data Protection Team at data@axcelera.co.uk.

17.4 All received SRFs will be handled by the Company's Data Protection Team.

17.5 The Company does not charge a fee for processing standard SRFs. However, the Company reserves the right to charge reasonable fees for additional copies of information already provided to an individual and for requests that are manifestly unfounded or excessive, particularly in cases of repetition.

17.6 All requests for copies of personal data will be fulfilled within one month of the individual's request. The period may be extended by up to two months for complex or numerous requests. If additional time is needed, the individual will be informed.

18. **Objections to Personal Data Processing**

18.1 Individuals have the right to object to the Company processing their personal data based on legitimate interests.

18.2 If an individual objects to the Company processing their personal data based on its legitimate interests, the Company will immediately cease such processing, unless it can be demonstrated that the Company's legitimate grounds for processing override the individual's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3 If an individual objects to the Company processing their personal data for direct marketing purposes, the Company will cease such processing immediately.

18.4 If an individual objects to the Company processing their personal data for scientific and/or historical research and statistical purposes, the individual must, under the GDPR, "demonstrate grounds relating to his or her particular situation."

18.5 Individuals wishing to make a data objection should do so using a Subject Request Form (SRF) and sending the form to the Company's Data Protection Team at data@axcelera.co.uk.

18.6 All received SRFs will be handled by the Company's Data Protection Team.

18.7 The Company does not charge a fee for processing standard SRFs. However, the Company reserves the right to charge reasonable fees for additional copies of information already provided to an individual and for requests that are manifestly unfounded or excessive, particularly in cases of repetition.

19. **Automated Decision-Making**

19.1 The Company presently does not utilise automated means for processing personal data. If it were to do so;

19.2 In cases where such decisions had a legal (or similarly significant) impact on data subjects, those individuals would possess the right, under the GDPR, to contest such decisions. They can request human intervention, present their own viewpoint, and seek an explanation of the decision from the Company.

19.3 The right outlined in Part 19.2 is not applicable in the following situations:

19.3.1 The decision is necessary for entering into, or fulfilling, a contract between the Company and the data subject;

19.3.2 The decision is authorised by law; or

19.3.3 The data subject has provided explicit consent.

20. **Profiling**

20.1 The Company currently refrains from using personal data for profiling purposes. If the Company were to do so;

20.2 In instances where personal data was utilised for profiling purposes, the following conditions would be applicable:

20.2.1 Data subjects would receive clear information explaining the profiling, including the significance and likely consequences of the profiling;

20.2.2 Appropriate mathematical or statistical procedures would be employed;

20.2.3 Technical and organisational measures would be enacted to minimise the risk of errors. If errors occurred, such measures would facilitate easy correction; and

20.2.4 All personal data processed for profiling purposes would be safeguarded to prevent discriminatory effects arising from profiling (refer to Parts 22 to 26 of this Policy for more details on data security).

21. **Personal Data Collected, Held, and Processed**

In accordance with the Data Retention Schedule, the Company collects, holds, and processes personal data (for information on data retention, kindly consult the Company's Data Retention Policy). The Data Retention Schedule is an integral component of the Directory of Data, Assets, Risk, Systems & Retention Schedule.

22. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure the implementation of the following measures for all communications and other transfers involving personal data:

22.1 All emails containing personal data must be sent from the AXCELERA Outlook or the client's email address.

22.2 Personal data may only be transmitted over secure networks; transmission over unsecured networks is not permitted under any circumstances.

22.3 When transferring personal data in hardcopy form, it should be handed directly to the recipient. If sent via post and unable to fit through a standard letterbox, it must be dispatched using a signed-for delivery service.

22.4 All physically transferred personal data, whether in hardcopy form or on removable electronic media, shall be conveyed in a suitable container marked as "confidential."

23. **Data Security – Storage**

The Company shall ensure the implementation of the following measures concerning the storage of personal data:

23.1.1 All electronic copies of personal data should be securely stored using AXCELERA systems. Hardcopies ('hard data') of personal data should be securely stored in a locked box, drawer, cabinet, or a similar secure facility.

23.1.2 All electronically stored personal data should be backed up in accordance with the Data Security Policy. All backups must be encrypted, following the guidelines outlined in the Data Security Policy.

23.1.3 Personal data should not be stored on any mobile device, including but not limited to laptops, tablets, and smartphones, except on AXCELERA authorised systems as per the Directory of Data, Assets, Risk, Systems & Retention Schedule. This applies to devices belonging to the Company or any other party.

23.1.4 Personal data should not be transferred to any personally owned device of team members, consultants, agents, contractors, and/or employees. Personal data may only be transferred to devices owned by agents, contractors, or other parties working on behalf of the Company if the concerned party has agreed to fully comply with the provisions of this Policy and the GDPR. This agreement may involve demonstrating to the Company that all appropriate technical and organisational measures have been taken.

24. **Data Security - Disposal**

When disposing of personal data for any reason, including instances where copies are no longer required, it must be securely deleted and disposed of. For additional details on the deletion and disposal of personal data, kindly refer to the Company's Data Retention Policy.

25. **Data Security - Use of Personal Data**

The Company will ensure the implementation of the following measures regarding the use of personal data:

25.1 Informal sharing of personal data is prohibited. If an employee, team member, consultant, agent, subcontractor, or any other party working on behalf of the Company requires access to personal data not already accessible to them, formal permission should be sought from the Data Protection Team via email at data@axcelera.co.uk.

25.2 Transfer of personal data to any individuals, including employees, team members, consultants, agents, contractors, or other parties, whether working on behalf of the Company or not, requires authorisation from the Data Protection Team via email at data@axcelera.co.uk.

25.3 Personal data must be handled with care, and it should not be left unattended or visible to unauthorised individuals, including employees, agents, subcontractors, or other parties.

25.4 When personal data is displayed on a computer screen, and the computer is to be left unattended, the user must lock the computer and screen before leaving.

25.5 The Data Protection Team is responsible for ensuring that appropriate consent is obtained, if required, and that no data subjects have opted out, whether directly or through a third-party service, for the personal data held by the Company.

26. **Data Security - IT Security**

26.1 All passwords used to safeguard personal data must avoid easily guessable words or phrases and must incorporate a combination of letters, numbers, and, where feasible, symbols.

26.2 Passwords must not be written down or shared among employees, agents, contractors, or other parties working on behalf of the Company, regardless of their position. Forgotten passwords must be reset using the applicable method.

26.3 All software, including applications and operating systems, should be kept up-to-date. Individuals, including employees, team members, consultants, agents, and contractors, are responsible for promptly installing security-related updates, unless valid technical reasons prevent doing so.

26.4 Installation of any software on Company-owned computers or devices requires prior approval from the CEO. Additional details on Data Security are available in the comprehensive Data Security Policy.

27. **Organisational Measures**

The Company will implement the following measures concerning the collection, holding, and processing of personal data:

27.1 Users will be fully briefed on their individual and Company responsibilities under the GDPR and this Policy, with a copy of this Policy provided to each.

27.2 Access to personal data held by the Company will be restricted to Users requiring it for their designated duties.

27.3 Users handling personal data will receive appropriate training.

27.4 Supervision of Users handling personal data will be ensured.

27.5 Users will exercise care and discretion when discussing work-related matters related to personal data.

27.6 Regular evaluation and review of methods for collecting, holding, and processing personal data will be conducted.

27.7 Periodic reviews of all personal data held by the Company will be performed, aligning with the Data Retention Policy.

27.8 The performance of Users handling personal data will be subject to regular evaluation.

27.9 Users handling personal data will be contractually bound to comply with GDPR principles.

27.10 Users will ensure that their employees/team members/consultants adhere to the conditions of this Policy and the GDPR. Failure to comply will require indemnification of the Company against any resulting costs, liability, damages, loss, claims, or proceedings.

28. **Transferring Personal Data to a Country Outside the UK**

28.1 The Company may transfer personal data to countries outside the UK.

28.2 Transfer of personal data will only occur if one or more of the following conditions are met:

- The country ensures an adequate level of protection for personal data.
- Appropriate safeguards are in place, including legally binding agreements, binding corporate rules, or standard data protection clauses.
- Informed consent is obtained from the data subject(s).
- The transfer is necessary for contractual performance, legal claims, public interest, vital interests, or public register access under UK law.

29. **Data Breach Notification**

29.1 All personal data breaches must be promptly reported to the Company's Data Protection Team.

29.2 If a breach poses a risk to data subjects' rights and freedoms, the Information Commissioner's Office must be informed within 72 hours of becoming aware of the breach.

29.3 For breaches likely to result in a high risk, affected data subjects must be directly and promptly informed by the Data Protection Team.

29.4 Data breach notifications shall include:

- Categories and approximate number of affected data subjects.
- Categories and approximate number of personal data records involved.
- Names and contact details of the Data Protection Team.
- Likely consequences of the breach.
- Details of measures taken or proposed to address and mitigate the breach's effects.

30. **Terms and Conditions**

The Company
Axcelera Ltd (Axcelera), a company registered in England under number 15353435, whose registered office is at 124 City Road, London, United Kingdom, EC1V 2NX

Data Controller
The entity determining the purposes, conditions, and means of processing personal data.

Data Processor
The entity processing data on behalf of the Data Controller.

Data Protection Authority
National authorities responsible for data and privacy protection, monitoring, and enforcing data protection regulations within the Union.

Data Protection Team (DPT)
A team of data privacy experts working independently to ensure adherence to GDPR policies and procedures.

Data Subject
A natural person whose personal data is processed by a controller or processor.

General Data Protection Regulation (GDPR)
The GDPR (Regulation (EU) 2016/679) is a regulation aiming to strengthen and unify data protection for individuals within the European Union (EU) and address the export of personal data outside the EU.

Hard data
Non-electronic stored data, including but not limited to printed data on paper.

Personal Data
Any information related to a natural person or 'Data Subject,' enabling direct or indirect identification.

Privacy Impact Assessment
A tool to identify and reduce privacy risks by analysing processed personal data and the policies in place to protect it.

Processing
Any operation on personal data, whether automated or not, including collection, use, recording, etc.

Profiling
Automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation
A binding legislative act applicable in its entirety across the Union.

Soft data
Electronically stored data.

Subject Access Right
Also known as the Right to Access, it entitles the data subject to access and information about their personal data held by a controller.

The User
Team members, consultants, agents, contractors, and/or employees, including part-time, temporary, or contract employees.

31. **Implementation of Policy**

This Policy shall be deemed effective as of 23rd December 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

32. **Related legislation**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

33. **Feedback and suggestion**

Users may provide feedback and suggestions about this document by emailing contact@axcelera.co.uk.

34. **SCHEDULE 1**

AXCELERA Ltd (AXCELERA)
Lawful Processing Summary

Explaining the legal bases we rely on

The law on data protection outlines various reasons for which a company may collect and process your personal data, including:

34.1 Consent
In specific situations, we can collect and process your data with your consent. For instance, if you (as a team member, consultant, agent, contractor, and/or employee) sign a Photo & Bio Consent Form for us to feature your photo on our website or if you (as a client) sign a Case Study or Testimonial Consent Form to showcase your case study or testimonial on our website.

34.2 Contractual Obligations
In certain circumstances, we need your personal data to fulfil our contractual obligations. For example, if you are a team member, consultant, agent, contractor, and/or employee, we would retain your contact details based on your employment contract. Similarly, if you are a client, your contact details would be kept on the client engagement letter.

34.3 Legal Compliance
If the law mandates, we may need to collect and process your data. For instance, we can share details of individuals involved in fraud or other criminal activities affecting AXCELERA with law enforcement. Additionally, if you are a team member, consultant, agent, contractor, and/or employee, we retain your tax details for legal compliance with HMRC.

34.4 Legitimate Interest
In specific situations, we may need your data to pursue our legitimate interests in a manner that could reasonably be expected as part of running our business and does not significantly impact your rights, freedom, or interests. For example, if you are a client or potential client, we will use your contact details to send you direct marketing information about products and services that we believe might interest you. If you are a team member, consultant, agent, contractor, and/or employee, we will also use your contact details to provide you with updates and information relevant to you.